

# Chebotarev Sets

Hershy Kisilevsky, Michael O. Rubinstein \*

March 13, 2012

## Abstract

We consider the problem of determining whether a set of primes, or, more generally, prime ideals in a number field, can be realized as a finite union of residue classes, or of Frobenius conjugacy classes. We give criteria for a set to be realized in this manner, and show that the subset of primes consisting of every other prime cannot be expressed in this way, even if we allow a finite number of exceptions.

## 1 Introduction

In this paper, we consider the following problem, and its generalizations:

Let  $p_n$  denote the  $n$ -th prime,  $\pi$  the set of all primes, and  $P_{\text{odd}}$  the set consisting of every other prime:

$$P_{\text{odd}} = \{p_n \in \pi | n \text{ odd}\} = \{2, 5, 11, 17, 23, \dots\}. \quad (1.1)$$

Can the set  $P_{\text{odd}}$  be realized as a finite union of primes in residue classes, even if we are willing to allow a finite number of exceptions, either in excess or deficiency?

---

\*Support for work on this paper was provided by the National Science Foundation under awards DMS-0757627 (FRG grant), and NSERC Discovery Grants

More generally, what about other sets of primes with rational density relative to the full set of primes? Is there an easy way to tell whether such a union is possible or not?

And what if, rather than just using, as our building blocks, primes in residue classes, we are permitted to take subsets of prime ideals that arise in the Chebotarev density theorem, i.e. of Frobenius conjugacy classes in the Galois groups of finite Galois extensions of  $\mathbb{Q}$ .

The natural instinct is that the set  $P_{\text{odd}}$  above cannot be realized in this manner. In fact, the number of subsets of primes with density  $1/2$  is uncountable, for example we can pick subsets by performing a random coinflip at each prime, yet the number of residue classes (or, more generally, Frobenius conjugacy classes) is countable. Therefore, most subsets of primes will fail to arise from residue or conjugacy classes.

However, how can one prove for a specific subset, such as  $P_{\text{odd}}$ , that it cannot be realized as a finite union of primes in residue/conjugacy classes, even if we are willing to allow a finite number of exceptions.

We will show, by contradiction, that the set  $P_{\text{odd}}$  is too ‘quiet’ relative to the set of all primes to arise on its own from genuine arithmetic sets. Primes in progressions, or in Frobenius conjugacy classes are very noisy and irregular, as a result of the non-trivial zeros of the  $L$ -functions that govern them.

More generally, one can ask similar question about subsets of prime ideals in an algebraic number field with rational density. This leads to our notion of Chebotarev sets.

## 1.1 Chebotarev Sets

Let  $K$  be a global field, and let  $\pi(K)$  denote the set of all non-zero prime ideals of  $K$ . Let  $L/K$  be a finite Galois extension of global fields with Galois group  $\text{Gal}(L/K) = G$ . If  $C \subset G$  is a conjugacy class in  $G$ , let  $P_{L/K,C}$  denote the set of primes  $\mathfrak{p} \in \pi(K)$  such that  $\mathfrak{p}$  is unramified in  $L/K$  and such that the conjugacy class  $(L/K, \mathfrak{p})$  of Frobenius automorphisms of primes  $\mathfrak{P} \in \pi(L), \mathfrak{P} \mid \mathfrak{p}$  is equal to  $C$ .

For two sets  $S_1, S_2$  the symmetric difference  $S_1 \triangle S_2$  is the set  $S_1 \setminus S_2 \cup S_2 \setminus S_1$ .

**Definition 1** *Call a set of primes  $P \subseteq \pi(K)$  a Chebotarev set for  $K$  if there are finitely many finite Galois extensions  $L_i/K$  and conjugacy classes  $C_i \subset \text{Gal}(L_i/K)$  such that  $P = \cup_i P_{L_i/K, C_i}$  up to finite sets. That is  $P \triangle \cup_i P_{L_i/K, C_i}$  is finite.*

Suppose that  $K \subseteq L' \subseteq L$  is a tower of finite extensions with  $L'/K$  and  $L/K$  both Galois. Then a conjugacy class in  $\text{Gal}(L'/K)$  can be lifted to a finite union of conjugacy classes in  $\text{Gal}(L/K)$ . Hence  $P$  is a Chebotarev set for  $K$  if and only if there is a finite Galois extension  $L/K$  and a finite number of conjugacy classes  $C_i \subset \text{Gal}(L/K)$  such that  $P = \cup_i P_{L/K, C_i}$  up to finite sets.

Given a Chebotarev set  $P \subseteq \pi(K)$  it follows from the Chebotarev density theorem that  $P$  has positive rational density, either Dirichlet density or natural density, or else has finitely many elements. Thus, any subset of  $\pi(K)$  with no density or irrational density cannot be a Chebotarev set.

Our problem is to produce a set  $P \subset \pi(K)$  of rational density

which is provably not a Chebotarev set. To this end, we have the following theorem.

**Theorem 1** *Let  $a/b \in \mathbb{Q}$ , with  $0 < a/b < 1$ . Assume that  $P$ , a subset of prime ideals in  $K$ , has rational density  $a/b$  in the set of all prime ideals  $\pi(K)$ , i.e.*

$$P(x) \sim \frac{a}{b} \pi(x, K), \quad (1.2)$$

where  $P(x)$  is the function which counts the number of elements in  $P$  and  $\leq x$ :

$$P(x) = \#\{\mathfrak{p} \in P \mid N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x\}. \quad (1.3)$$

Assume, further, that  $P$  is a Chebotarev set, i.e. there exists sets  $P_{L/K, C_j}$  of Frobenius conjugacy classes such that the symmetric difference

$$P \triangle \bigcup_{j=1}^r P_{L/K, C_j} \quad (1.4)$$

is finite (i.e. the exceptions). Then,

$$P(x) - \frac{a}{b} \pi(x, K) = \Omega\left(\frac{x^{1/2}}{\log x}\right). \quad (1.5)$$

with the implied constant in the  $\Omega$  depending on  $P$ .

Here, we are using the following definition of the  $\Omega$  notation. We say that

$$f(x) = \Omega(g(x))$$

if

$$\limsup |f(x)|/g(x) > 0,$$

i.e. if there exists a sequence  $x_n$  with  $x_n \rightarrow \infty$ , and a constant  $c > 0$  such that  $|f(x_n)| > cg(x_n)$ .

As we will explain in the proof of this theorem, the same result continues to hold if we replace the counting function  $\frac{a}{b}\pi(x, K)$  with  $\frac{a}{b}\pi(x, F)$ , where  $F$  is *any* algebraic number field, i.e.  $F$  can be different than  $K$ . We can also replace it with  $\frac{a}{b}\text{Li}(x)$ , or with the counting function  $Q(x)$  of another Chebotarev set  $Q$ , so long as  $Q$  has the same density,  $a/b$ , as  $P$  and is essentially distinct from  $P$ . By essentially distinct, we mean that the symmetric difference  $P \triangle Q$  is infinite.

**Theorem 2** *Let  $P$  and  $a/b$  be as in the previous theorem, and  $f(x)$  stand for any of  $\frac{a}{b}\text{Li}(x)$ ,  $\frac{a}{b}\pi(x, F)$ , or  $Q(x)$ , as defined above. Then*

$$P(x) - f(x) = \Omega\left(\frac{x^{1/2}}{\log x}\right), \quad (1.6)$$

*with the implied constant depending on  $P$  and  $f$ .*

A slightly more general form of our theorem allows one to consider a summatory function on prime ideals of  $K$  with complex valued weight function that is constant on Frobenius conjugacy classes of  $G$ :

**Theorem 3** *Define*

$$F(x) := \sum \pi(x, L/K, C_j) \lambda_j, \quad (1.7)$$

*where  $\lambda_j \in \mathbb{C}$ , and is assumed to satisfy  $\sum |\lambda_j| \neq 0$ . The sum is over the distinct conjugacy classes  $C_j$  of  $G = \text{Gal}(L/K)$ , and  $\pi(x, L/K, C_j)$  is defined in (3.2). Let*

$$\lambda := \frac{1}{|G|} \sum \lambda_j |C_j|. \quad (1.8)$$

*Then*

$$F(x) - \lambda \text{Li}(x) = \Omega\left(\frac{x^{1/2}}{\log x}\right), \quad (1.9)$$

*with the implied constant depending on  $F$ , and  $\lambda_j$ .*

For example, we can recover Theorem 1 by taking  $\lambda_j = 1 - a/b$  for  $1 \leq j \leq r$ , and  $-a/b$  otherwise. Observe, in this example, that  $\lambda = 0$ , so that no  $Li(x)$  term appears.

The key idea used to prove these theorems is that the functions on the lhs of (1.5) (1.6), and (1.9) are discontinuous on a positive proportion of  $N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x$ . Consequently, when expressed as a linear combination of explicit formulas, infinitely many of the non-trivial zeros of the relevant  $L$ -functions must survive. These zeros are responsible for making these differences large on average, which we show by considering their mean square on a logarithmic scale.

Note that the statements of Theorems 1- 3 do not assume the Generalized Riemann Hypothesis. In fact, if the GRH does not hold, a stronger  $\Omega$  result than (1.5) holds, hence we have stated these theorems unconditional on the GRH.

The precise statement of the  $\Omega$  bound in the case that the GRH fails requires some discussion concerning the location of the zeros of the relevant  $L$ -functions, and how these zeros interact upon taking certain linear combinations of the logarithmic derivatives of these  $L$ -functions. This discussion and corresponding result can be found in Section 2.2 and in Theorem 4 at the end of Section 3.1.

Therefore, to rule out a set  $P$  as being Chebotarev, one need only show that either Theorem 1 or 2 is violated. So, for example, the set  $P_{\text{odd}}$  specified in the introduction of density  $1/2$  in the rational primes, consisting of every other prime, cannot be realized as a Chebotarev set. We can prove this by considering the counting function  $P_{\text{odd}}(x)$ , equal to the number of elements in  $P_{\text{odd}}$  and  $\leq x$ :

$$P_{\text{odd}}(x) = \#\{p \in P_{\text{odd}} | p \leq x\}. \quad (1.10)$$

Because  $P_{\text{odd}}$  counts every other prime, we have that

$$P_{\text{odd}}(x) - \pi(x)/2 = \begin{cases} 1/2, & \text{if } p_{2j-1} \leq x < p_{2j} \\ 0, & \text{if } p_{2j} \leq x < p_{2j+1}, \end{cases} \quad (1.11)$$

which violates Theorem 1. Hence  $P_{\text{odd}}$  cannot be realized as a Chebotarev set.

**Definition 2** *Call a set of primes  $P \subseteq \pi(K)$  an almost Chebotarev set for  $K$  if there is a Chebotarev set  $U$  such that  $P = U$  up to sets of density zero. That is  $P \triangle U$  has density zero.*

It seems much more difficult to produce a set which is provably not almost Chebotarev – although we suspect that our example,  $P_{\text{odd}}$ , is one such set.

We conclude the introduction by noting that Serre studied ‘Frobenian’ (i.e. named differently than here) sets and functions in his paper [8] and book [9] (see his Chapter 3), the latter in relation to the problem of counting the number of solutions mod  $p$  to a system of polynomial equations. Lagarias defined a similar notion of Chebotarev sets in [5], also for studying solutions to polynomial congruences modulo  $p$ . See Lemma 3.1 in his paper for the equivalence of his definition to ours, though without allowing for finitely many exceptions.

## 2 The classical case

In this section we consider the more classical situation of sets  $P$  of rational primes that are realized using residue classes. We will essentially establish Theorem 1 for the special case of residue classes, rather than Frobenius conjugacy classes.

The techniques that we develop will serve as a model, in Section 3, where we will modify our approach to the general setting of Chebotarev sets.

Assume that

$$P = P_0 \cup \bigcup_{j=1}^r P_{a_j, q_j} \setminus P_1 \quad (2.12)$$

where  $P_0, P_1$  consists of finitely many elements, i.e. the possible exceptions in excess and deficiency, and

$$P_{a,q} = \{p \in \pi \mid p \equiv a \pmod{q}\} \quad (2.13)$$

consists of primes in the residue class  $a \pmod{q}$ .

We can simplify a bit and assume that all the  $q_j$  are equal, since, if not, we could simply rewrite (2.12) in terms of the least common multiple of the  $q_j$  and take additional residue classes as needed. For example, the set of primes that are  $1 \pmod{4}$  union the primes that are  $5 \pmod{6}$  is equivalent to the set of primes that are  $1, 5, 11 \pmod{12}$ .

Thus we are assuming the existence of a single positive integer  $q$ , and distinct residue classes  $a_j \pmod{q}$  such that, after relabelling  $r$  as needed,

$$P = P_0 \cup \bigcup_{j=1}^r P_{a_j, q} \setminus P_1. \quad (2.14)$$

We can also assume that  $\gcd(a_j, q) = 1$ .

We consider the counting function  $P(x)$  which is equal to the number of elements in  $P$  and  $\leq x$ :

$$P(x) = \#\{p \in P \mid p \leq x\}. \quad (2.15)$$

Next, we define, as usual,

$$\pi(x, q, a) = \#\{p \leq x \mid p \equiv a \pmod{q}\}. \quad (2.16)$$



From equation (2.14), we have, for  $x$  larger than all of the elements of  $P_0$  and  $P_1$ , that

$$P = \lambda + \sum_{j=1}^r \pi(x, q, a_j), \quad (2.17)$$

where

$$\lambda = |P_0| - |P_1|. \quad (2.18)$$

The prime number theorem which states that

$$\pi(x) \sim \text{Li}(x), \quad (2.19)$$

where

$$\text{Li}(x) = \int_2^x dt / \log t \sim \frac{x}{\log x}. \quad (2.20)$$

The prime number theorem for arithmetic progressions, proven by Hadamard and de la Vallée Poussin, asserts, for  $\gcd(a, q) = 1$ , that primes are equidistributed amongst the residue classes mod  $q$  that are relatively prime to  $q$ :

$$\pi(x, q, a) \sim \frac{\pi(x)}{\phi(q)}, \quad (2.21)$$

where  $\phi(q) = \#\{a \bmod q \mid (a, q) = 1\}$ . Therefore,

$$P(x) \sim \frac{r}{\phi(q)} \pi(x). \quad (2.22)$$

We also make the assumption that

$$\frac{r}{\phi(q)} < 1, \quad (2.23)$$

so that  $P$  omits a positive proportion of the primes.

## 2.1 Explicit formula

One can write an explicit formula for  $\pi(x, q, a)$  in terms of the zeros of the Dirichlet  $L$ -functions,  $L(s, \chi)$ , where  $\chi$  runs over all Dirichlet characters for the modulus  $q$ .

For a given  $q$ , let  $\chi$  be a Dirichlet character modulo  $q$ . We will denote the principal character by  $\chi_0$ . Let

$$\psi(x, \chi) := \sum_{n \leq x} \chi(n) \Lambda(n) \quad (2.24)$$

where  $\Lambda(n) = \log p$  if  $n = p^m$  for some  $m \in \mathbb{Z}$ , and is 0 otherwise.

The explicit formula for  $\pi(x, q, a)$  can be derived from that of

$$\begin{aligned} \psi(x, q, a) &:= \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n) \\ &= \frac{1}{\phi(q)} \sum_{\chi \pmod{q}} \bar{\chi}(a) \sum_{n \leq x} \Lambda(n) \chi(n) \\ &= \frac{1}{\phi(q)} \sum_{\chi \pmod{q}} \bar{\chi}(a) \psi(x, \chi). \end{aligned} \quad (2.25)$$

The main contribution to  $\psi(x, q, a)$  comes from the principal character:

$$\psi(x, \chi_0) = \sum_{\substack{p^k \leq x \\ p \nmid q}} \log(p) = \psi(x) - \sum_{\substack{p^k \leq x \\ p \mid q}} \log(p). \quad (2.26)$$

Therefore

$$\psi(x, q, a) = \frac{1}{\phi(q)} \left( \psi(x) + \sum_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} \bar{\chi}(a) \psi(x, \chi) - \sum_{\substack{p^k \leq x \\ p \mid q}} \log(p) \right). \quad (2.27)$$

We define

$$\begin{aligned} \Pi(x, q, a) &:= \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \frac{\Lambda(n)}{\log(n)} = \sum_{\substack{p^k \leq x \\ p^k \equiv a \pmod{q}}} \frac{1}{k} \\ &= \pi(x, q, a) + R(x, q, a) \end{aligned} \quad (2.28)$$

with

$$R(x, q, a) = \sum_{\substack{p^k \leq x \\ k \geq 2 \\ p^k \equiv a \pmod{q}}} \frac{1}{k}. \quad (2.29)$$

Therefore,

$$\pi(x, q, a) = \Pi(x, q, a) - R(x, q, a). \quad (2.30)$$

Now, summing by parts

$$\Pi(x, q, a) = \frac{\psi(x, q, a)}{\log(x)} + \int_2^x \frac{\psi(t, q, a)}{t \log(t)^2} dt, \quad (2.31)$$

so that

$$\pi(x, q, a) = \frac{\psi(x, q, a)}{\log(x)} + \int_2^x \frac{\psi(t, q, a)}{t \log(t)^2} dt - R(x, q, a). \quad (2.32)$$

Substituting (2.25) into the above, we get

$$\begin{aligned} \pi(x, q, a) = & \frac{1}{\phi(q)} \left( \frac{\psi(x)}{\log(x)} + \int_2^x \frac{\psi(t)}{t \log(t)^2} dt - \frac{\sum_{\substack{p^k \leq x \\ p|q}} \log(p)}{\log(x)} - \int_2^x \frac{\sum_{\substack{p^k \leq t \\ p|q}} \log(p)}{t \log(t)^2} dt \right) \\ & + \frac{1}{\phi(q)} \sum_{\substack{\chi \bmod q \\ \chi \neq \chi_0}} \bar{\chi}(a) \left( \frac{\psi(x, \chi)}{\log(x)} + \int_2^x \frac{\psi(t, \chi)}{t \log(t)^2} dt \right) - R(x, q, a). \end{aligned} \quad (2.33)$$

The special case of  $q = 1$  (and any value for  $a$ ) of (2.32) is:

$$\pi(x) = \frac{\psi(x)}{\log(x)} + \int_2^x \frac{\psi(t)}{t \log(t)^2} dt - R(x, 1), \quad (2.34)$$

with

$$R(x, 1) = \sum_{k \geq 2} \frac{\pi(x^{1/k})}{k}. \quad (2.35)$$

With these formulas in hand, consider again the difference  $P(x) - \frac{r}{\phi(q)} \pi(x)$ . Subtracting  $\frac{r}{\phi(q)} \pi(x)$  from (2.17), and then substituting (2.33)

and (2.34) gives:

$$\begin{aligned}
P(x) - \frac{r}{\phi(q)}\pi(x) &= \lambda + \sum_{j=1}^r \pi(x, q, a_j) - \frac{r}{\phi(q)}\pi(x) \\
&= \lambda + \sum_{\substack{\chi \bmod q \\ \chi \neq \chi_0}} c_\chi \left( \frac{\psi(x, \chi)}{\log(x)} + \int_2^x \frac{\psi(t, \chi)}{t \log(t)^2} dt \right) + \frac{rR(x, 1)}{\phi(q)} - \sum_{j=1}^r R(x, q, a_j) \\
&\quad - \frac{r}{\phi(q)} \left( \frac{\sum_{\substack{p^k \leq x \\ p|q}} \log(p)}{\log(x)} + \int_2^x \frac{\sum_{\substack{p^k \leq t \\ p|q}} \log(p)}{t \log(t)^2} dt \right), \tag{2.36}
\end{aligned}$$

where

$$c_\chi = \frac{1}{\phi(q)} \sum_{j=1}^r \bar{\chi}(a_j). \tag{2.37}$$

Note above, that, on summing over  $r$  values of  $a_j$  and subtracting  $r/\phi(q)$  times (2.34), we cancelled the main term

$$\frac{r}{\phi(q)} \left( \frac{\psi(x, \chi)}{\log(x)} + \int_2^x \frac{\psi(t, \chi)}{t \log(t)^2} dt \right). \tag{2.38}$$

We will show that the rhs of (2.36) can get as large, in absolute value, as  $\gg x^{1/2}/\log(x)$ . This will be independent of the GRH. In fact, if GRH fails, the lower bound that we can prove is at least as large.

The classic explicit formula for  $\psi(x, \chi)$ , where  $\chi \neq \chi_0$  is a primitive character, takes the form, for  $x > 1$  not a prime power,

$$\psi(x, \chi) = - \sum_{\rho_\chi} \frac{x^{\rho_\chi}}{\rho_\chi} - (1 - \mathfrak{a}_\chi) \log x - b(\chi) + \sum_{m=1}^{\infty} \frac{x^{\mathfrak{a}_\chi - 2m}}{2m - \mathfrak{a}_\chi}, \tag{2.39}$$

where  $\rho_\chi$  runs over the non-trivial zeros of  $L(s, \chi)$ , with the sum over zeros taken as  $\lim_X \rightarrow \infty |\Im \rho_\chi| < X$ . Also,  $\mathfrak{a}_\chi = 1$  if  $\chi(-1) = -1$  and 0 otherwise, and  $b(\chi)$  is a constant depending on  $\chi$ , namely the constant term in the Laurent expansion about  $s = 0$  of  $L'/L(s, \chi)$  (Taylor expansion if  $\chi(-1) = -1$ ). If  $x$  is a prime power, the rhs

above converges to  $\psi(x, \chi) - \Lambda(x)\chi(x)/2$ , i.e. one needs to subtract half of the last term in the sum defining  $\psi(x, \chi)$ . For a derivation of this explicit formula see, for instance, Davenport [2, pgs 115-120].

When  $\chi$  is an imprimitive character, say induced by  $\chi_1 \bmod q_1$ , then

$$\psi(x, \chi) = \psi(x, \chi_1) - \sum_{\substack{p^k \leq x \\ p \nmid q}} \log(p) \chi_1(p^k). \quad (2.40)$$

For notational convenience, in the case of imprimitive  $\chi$ , we set  $\mathfrak{a}_\chi = \mathfrak{a}_{\chi_1}$  and also  $b(\chi) = b(\chi_1)$ .

Therefore, we can rewrite (2.36) in the following form:

$$P(x) - \frac{r}{\phi(q)} \pi(x) = \frac{1}{\log x} \sum_{\rho} \alpha_{\rho} \frac{x^{\rho}}{\rho} + A(x) + B(x), \quad (2.41)$$

where  $\alpha_{\rho} \in \mathbb{C}$  and the sum over  $\rho$  is taken over the union over the non-trivial zeros of all  $L(s, \chi)$ ,  $\chi \bmod q$ . We may assume that the  $\rho$  in the sum are distinct, by grouping equal  $\rho$  under the same  $\alpha_{\rho}$ . In the case of imprimitive characters, the non-trivial zeros of  $L(s, \chi)$  coincide with those of the Dirichlet  $L$ -function,  $L(s, \chi_1)$ , corresponding to the inducing character  $\chi_1$ . Also observe that

$$\alpha_{\rho} = O_q(1) \quad (2.42)$$

as the  $\alpha_{\rho}$ 's are obtained by taking the linear combination  $\sum_{\chi \neq \chi_0} c_{\chi} \psi(x, \chi)$ , and then grouping together equal  $\rho$  (if there are any. Distinct  $L(s, \chi)$ , for primitive  $\chi$ , presumably have distinct non-trivial zeros).

The function  $A(x)$  gathers together all the remaining terms that

are discontinuous:

$$\begin{aligned}
A(x) &= \frac{rR(x, 1)}{\phi(q)} - \sum_{j=1}^r R(x, q, a_j) - \frac{r}{\phi(q)} \frac{\sum_{\substack{p^k \leq x \\ p|q}} \log(p)}{\log(x)} \\
&\quad - \frac{1}{\log x} \sum_{\substack{\chi \pmod q \\ \chi \neq \chi_0 \\ \chi \text{ imprimitive}}} c_\chi \sum_{\substack{p^k \leq x \\ p|q}} \log(p) \chi_1(p^k), \tag{2.43}
\end{aligned}$$

and  $B(x)$  incorporates the rest:

$$\begin{aligned}
B(x) &= \lambda - \frac{r}{\phi(q)} \int_2^x \frac{\sum_{\substack{p^k \leq t \\ p|q}} \log(p)}{t \log(t)^2} dt + \sum_{\substack{\chi \pmod q \\ \chi \neq \chi_0}} c_\chi \left( \int_2^x \frac{\psi(t, \chi)}{t \log(t)^2} dt \right. \\
&\quad \left. - (1 - \mathfrak{a}_\chi) + \frac{b(\chi)}{\log x} - \frac{1}{\log x} \sum_{m=1}^{\infty} \frac{x^{\mathfrak{a}_\chi - 2m}}{2m - \mathfrak{a}_\chi} \right). \tag{2.44}
\end{aligned}$$

Notice that  $A(x)$  has jump discontinuities at a relatively thin set of prime powers:  $R(x, 1)$  and  $R(x, q, a_j)$  jump when  $x$  is a prime power  $p^k$  with  $k \geq 2$ . The remaining terms in  $A(x)$  jump at prime powers  $p^k$  with  $p|q$ ,  $k \geq 1$ . Hence, overall,  $A(x)$  has only finitely many jump discontinuities at the primes, namely the primes  $p$  that divide  $q$ . Furthermore every term that appears in  $B(x)$  is continuous with respect to  $x$ . But  $P(x) - \frac{r}{\phi(q)}\pi(x)$  is discontinuous at all primes (our assumption that  $r/\phi(q) < 1$  enters here).

Therefore, the sum over  $\rho$  in (2.41) must have infinitely many terms with  $\alpha_\rho \neq 0$ , otherwise the sum over  $\rho$  would be continuous a function for all  $x$ .

The fact that at least one  $\alpha_\rho$  is non-zero is a crucial point, and we are now in a position to obtain our  $\Omega$  results.

Let  $\Theta$  be the lim sup of the real parts of the zeros  $\rho$  such that  $\alpha_\rho \neq 0$ , i.e. the zeros that appear in (2.41):

$$\Theta = \limsup \{\Re \rho | \alpha_\rho \neq 0\}. \tag{2.45}$$

Equivalently, from (2.36),  $\Theta$  is the lim sup of the poles of the function

$$-\sum_{\chi \neq \chi_0} c_\chi \frac{L'(s, \chi)}{L(s, \chi)} + \frac{r}{\phi(q)} \frac{\zeta'(s)}{\zeta(s)}, \quad (2.46)$$

and also of the singularities of

$$\sum_{\chi \neq \chi_0} c_\chi \log(L(s, \chi)) - \frac{r}{\phi(q)} \log(\zeta(s)). \quad (2.47)$$

Notice that  $\Theta \geq 1/2$ , since the zeros of  $L(s, \chi)$  that occur off the half line (assuming GRH fails) come in pairs,  $\rho$  and  $1 - \bar{\rho}$ , symmetric about the line  $\Re s = 1/2$ .

## 2.2 $\Omega$ bound, assuming $\Theta > 1/2$

We first assume that  $\Theta > 1/2$ , i.e. that the GRH fails and that at least one zero to the right of  $\Re(s) = 1/2$  survives in the explicit formula on taking the linear combination in (2.36).

We will prove that, for every  $\delta > 0$ ,

$$P(x) - \frac{r}{\phi(q)} \pi(x) = \Omega(x^{\Theta-\delta}), \quad (2.48)$$

with the implied constant depending on  $\delta$  and  $q$ , by establishing, assuming  $\Theta > 1/2$ , the estimate

$$\sum_{j=1}^r \Pi(x, q, a_j) - \frac{r}{\phi(q)} \Pi(x) = \Omega(x^{\Theta-\delta}). \quad (2.49)$$

The above is easier to work with than (2.48), since  $L$ -functions naturally count prime powers rather than just primes. Notice that, because  $\Pi(x, q, a) - \pi(x, q, a) = O_q(x^{1/2}/\log(x))$  and  $\Pi(x) - \pi(x) = O(x^{1/2}/\log(x))$  (see (2.54) and (2.55) below) so that, by choosing  $0 < \delta < \Theta - 1/2$ , we have that (2.49) implies (2.48) (and then for every  $\delta > 0$ , since taking  $\delta$  larger gives a weaker bound).

Argue by contradiction. Assume that (2.49) does not hold, i.e. that there exists a  $\delta > 0$  such that  $|\sum_{j=1}^r \Pi(x, q, a_j) - \frac{r}{\phi(q)} \Pi(x)| \ll x^{\Theta-\delta}$ . Consider the Dirichlet integral (akin to Dirichlet series, see Chapter 5 of [4]),

$$\begin{aligned} \int_1^\infty \frac{\sum_{j=1}^r \Pi(x, q, a_j) - \frac{r}{\phi(q)} \Pi(x)}{x^{s+1}} dx &= \frac{1}{s} \sum_{\chi} c_{\chi} \log(L(s, \chi)) - \frac{r}{s\phi(q)} \log(\zeta(s)) \\ &= \frac{1}{s} \sum_{\chi \neq \chi_0} c_{\chi} \log(L(s, \chi)) + \frac{r}{s\phi(q)} \sum_{p|q} \log(1 - p^{-s}). \end{aligned} \quad (2.50)$$

One can prove this identity, when  $\Re s > 1$ , by observing that the numerator of the integrand is a step function with steps at prime powers, and then integrating termwise the contribution from each prime power. The assumption that  $\Re s > 1$  is used to rearrange integration and summation and also to identify the resulting Dirichlet series with the rhs above.

Notice that the rhs above has singularities (branch cuts) coming from the zeros of  $L(s, \chi)$ , specifically from the  $\rho$  with  $\alpha_{\rho} \neq 0$  (and some additional singularities originating on the line  $\Re s = 0$ ).

Now, if the numerator of the above integrand is  $\ll x^{\Theta-\delta}$ , then the lhs of (2.50) defines an analytic function for  $\Re s > \Theta - \delta$ . But this contradicts, from the definition of  $\Theta$ , the fact that the rhs has singularities in this half plane. Therefore,

$$\sum_{j=1}^r \Pi(x, q, a_j) - \frac{r}{\phi(q)} \Pi(x) = \Omega(X^{\Theta-\delta}), \quad (2.51)$$

for all  $\delta > 0$ .



### 2.3 $\Omega$ estimate in the classical case, assuming $\Theta = 1/2$

In this subsection, we assume that  $\Theta = 1/2$ . This can occur in two ways: either if the GRH holds, or if the only zeros surviving the linear combination of explicit formulae arising from (2.36) are on the half line.

The above result can be improved when  $\Theta = 1/2$ . In that case we will show that

$$P(x) - \frac{r}{\phi(q)}\pi(x) = \Omega(x^{1/2}/\log(x)). \quad (2.52)$$

While we could modify the approach given in the previous subsection, it is complicated by the presence of the squares of primes. We could adapt the approach described in Ingham [4] for the problem of  $\psi(x) - x$ , and prove that

$$\sum_{j=1}^r \Pi(x, q, a_j) - \frac{r}{\phi(q)}\Pi(x) = \Omega_{\pm}(x^{1/2}/\log x), \quad (2.53)$$

i.e. that the difference of these prime power counting functions gets, in size, as large as a constant times  $x^{1/2}/\log x$ , and points in *both* positive and negative directions for infinite sequences of  $x \rightarrow \infty$ . Now the squares of primes contribute an amount to  $P(x) - \frac{r}{\phi(q)}\pi(x)$  that is asymptotically a constant times  $x^{1/2}/\log(x)$ , i.e. of the same size as (2.53), but always pointing in one direction. Hence, estimate (2.53) would establish (2.52).

Instead, however, we will take an alternate approach that yields more information. We will consider two mean square averages of the remainder term, each giving a separate proof of (2.52). Both averages are of interest in their own right.

We first bound each term that appears in  $A(x)$ ,  $B(x)$ . The prime number theorem and (2.35) give

$$R(x, 1) = \pi(x^{1/2})/2 + O(x^{1/3}/\log x) = x^{1/2}/\log x + O(x^{1/2}/\log(x)^2). \quad (2.54)$$

Similarly, from the prime number theorem for arithmetic progressions, we have

$$\sum_{j=1}^r R(x, q, a_j) = \kappa x^{1/2}/\log x + O_q(x^{1/2}/\log(x)^2), \quad (2.55)$$

with the implied constant in the  $O$  depending on  $q$ , and

$$\kappa = \frac{1}{\phi(q)} \sum_{j=1}^r \sum_{b^2=a_j \pmod q} 1. \quad (2.56)$$

Finally, there are only finitely many  $p|q$ . Furthermore,  $p^k \leq x$  implies that  $k \leq \log(x)/\log(p)$ . Hence  $\sum_{\substack{p^k \leq x \\ p|q}} \log(p) = O_q(\log x)$ , and so

$$-\frac{1}{2} \frac{\sum_{\substack{p^k \leq x \\ p|q}} \log(p)}{\log(x)} - \frac{1}{\log x} \sum_{\substack{\chi \pmod q \\ \chi \neq \chi_0 \\ \chi \text{ imprimitive}}} c_\chi \sum_{\substack{p^k \leq x \\ p|q}} \log(p) \chi_1(p^k) = O_q(1). \quad (2.57)$$

Putting these together gives

$$A(X) = (r/\phi(q) - \kappa)x^{1/2}/\log x + O_q(x^{1/2}/\log(x)^2). \quad (2.58)$$

To estimate  $B(x)$ , notice that

$$\int_2^x \frac{\sum_{\substack{p^k \leq t \\ p|q}} \log(p)}{t \log(t)^2} dt \ll_q \int_2^x \frac{dt}{t \log(t)} \ll \log \log x. \quad (2.59)$$

Thus, because  $\lambda$  and second line of (2.44) are bounded, we have

$$B(x) \ll_q \left| \sum_{\chi \neq \chi_0} c_\chi \int_2^x \frac{\psi(t, \chi)}{t \log(t)^2} dt \right| + \log \log x. \quad (2.60)$$

Let

$$G(x, \chi) = \int_2^x \psi(t, \chi) dt/t. \quad (2.61)$$

Equation (5), page 117, of Davenport [2] gives the explicit formula with a rate of convergence:

$$\psi(x, \chi) = - \sum_{|\Im \rho_\chi| < X} \frac{x^{\rho_\chi}}{\rho_\chi} + O_q(x \log(xX)^2/X + \log x), \quad (2.62)$$

valid for  $x \geq 2$  (or else for  $x > 1$  by adding a 1 to the  $O$ -term). Note that this formula, with the  $O(\log x)$  included, is true for both primitive and imprimitive characters, and whether  $x$  is equal to a prime power or not. We have also absorbed the last three terms of (2.39) into the  $O$  term above. Thus, integrating and letting  $X \rightarrow \infty$ , we have

$$G(x, \chi) = - \sum_{\rho_\chi} \frac{x^{\rho_\chi}}{\rho_\chi^2} + O_q(\log(x)^2). \quad (2.63)$$

The above series over  $\rho_\chi$  converges absolutely as can be seen from the asymptotic formula for the number of zeros [2, pg 101],

$$N(T, \chi) := \#\{|\Im \rho_\chi| \leq T\} = \frac{T}{\pi} \log \frac{qT}{2\pi} - \frac{T}{\pi} + O(\log T + \log q). \quad (2.64)$$

Summing over  $\chi$  we get

$$\sum_{\chi \neq \chi_0} c_\chi \int_2^x \frac{\psi(t, \chi)}{t} dt = - \sum_{\rho} \alpha_\rho \frac{x^\rho}{\rho^2} + O_q(\log(x)^2), \quad (2.65)$$

with the sum over all non-trivial zeros  $\rho$  of all  $L(s, \chi)$  for the modulus  $q$ . The same coefficients  $\alpha_\rho$  appear here as in (2.41) because the same linear combination of the terms involving the zeros  $\rho$  appears as in the sum  $\sum_{\chi \neq \chi_0} c_\chi \psi(x, \chi)$ .

It follows, on integrating by parts, that

$$\sum_{\chi \neq \chi_0} c_\chi \int_2^x \frac{\psi(t, \chi)}{t \log(t)^2} dt \ll_q \frac{x^{1/2}}{\log(x)^2} \sum_{\rho} \frac{|\alpha_\rho|}{|\rho|^2} \ll_q \frac{x^{1/2}}{\log(x)^2}. \quad (2.66)$$

Thus, returning to (2.60), we get

$$B(x) \ll_q \frac{x^{1/2}}{\log(x)^2}. \quad (2.67)$$

Thus, our estimates (2.58) and (2.67) for  $A(x)$  and  $B(x)$  give

$$P(x) - \frac{r}{\phi(q)}\pi(x) = \frac{1}{\log x} \left( \sum_{\rho} \alpha_{\rho} \frac{x^{\rho}}{\rho} + (r/\phi(q) - \kappa)x^{1/2} + O\left(x^{1/2}/\log x\right) \right), \quad (2.68)$$

By (2.62), for  $2 \leq x < X$ , we can write this as a finite sum over  $\rho$ :

$$P(x) - \frac{r}{\phi(q)}\pi(x) = \frac{x^{1/2}}{\log x} \left( \sum_{|\gamma| < X} \alpha_{\rho} \frac{x^{i\gamma}}{\rho} + (r/\phi(q) - \kappa) + O\left(\frac{x^{1/2} \log(X)^2}{X} + \frac{1}{\log x}\right) \right), \quad (2.69)$$

where  $\rho = 1/2 + i\gamma$ . The assumption  $x < X$  is simply used here to simplify, in (2.62),  $\log(xX)$  by  $\log X$ . We also use it below when estimating the contribution from the above  $O$  term.

Finally, we need to deal with the possibility of non-trivial zeros at  $s = 1/2$ . Such terms contribute a constant times  $x^{1/2}/\log x$  to the above, and we may rewrite it as:

$$P(x) - \frac{r}{\phi(q)}\pi(x) = \frac{x^{1/2}}{\log x} \left( \sum_{0 < |\gamma| < X} \alpha_{\rho} \frac{x^{i\gamma}}{\rho} + \nu + O\left(\frac{x^{1/2} \log(X)^2}{X} + \frac{1}{\log x}\right) \right), \quad (2.70)$$

where  $\nu$  is equal to  $r/\phi(q) - \kappa$  plus, if the term  $\rho = 1/2$  appears in the sum,  $2\alpha_{1/2}$ .

## 2.4 A mean square estimate of the average difference

Let

$$\Delta(x) := \frac{\log x}{x^{1/2}} \left( P(x) - \frac{r}{\phi(q)}\pi(x) \right). \quad (2.71)$$

Rather than work with  $\Delta(x)$  directly, it is technically easier to work with its average:

$$M(x) := \frac{1}{x} \int_2^x \Delta(t) dt = \sum_{\rho \neq 1/2} \alpha_\rho \frac{x^{i\gamma}}{\rho(i\gamma + 1)} + \nu + O(1/\log x). \quad (2.72)$$

The latter equality can be derived by integrating the bracketed expression in (2.70) termwise, and letting  $X \rightarrow \infty$ .

Formula (2.64) implies that  $\sum_\rho 1/(\rho(i\gamma + 1))$  converges absolutely, and this simplifies our analysis of the mean square. Indeed, we can truncate the above sum over  $\rho$  so that the tail is uniformly small. More precisely, for any  $\epsilon > 0$ , there exists  $T = T(\epsilon)$  such that

$$M(x) = \sum_{0 < |\gamma| < T} \alpha_\rho \frac{x^{i\gamma}}{\rho(i\gamma + 1)} + \nu + V(x), \quad (2.73)$$

where

$$V(x) < \epsilon, \quad (2.74)$$

for all  $x$  sufficiently large.

The natural scale at which to analyze the explicit formula is logarithmic. Set  $y = \log x$ , and consider

$$\frac{1}{Y} \int_{\log 2}^Y |M(e^y)|^2 dy \quad (2.75)$$

Substitute the rhs of (2.73) for  $M(e^y)$ . Now,

$$\begin{aligned} & \lim_{Y \rightarrow \infty} \frac{1}{Y} \int_{\log 2}^Y \left| \sum_{0 < |\gamma| < T} \alpha_\rho \frac{e^{i\gamma y}}{\rho(i\gamma + 1)} + \nu \right|^2 dy \\ &= \sum_{0 < |\gamma| < T} \frac{|\alpha_\rho|^2}{|\rho(i\gamma + 1)|^2} + \nu^2, \end{aligned} \quad (2.76)$$

which follows by multiplying

$$\sum_{0 < |\gamma| < T} \alpha_\rho \frac{e^{i\gamma y}}{\rho(i\gamma + 1)} + \nu \quad (2.77)$$

by its conjugate, expanding, and noting that only the diagonal terms survive the limit  $Y \rightarrow \infty$ . Next, the expression in (2.77) is bounded for  $y \in \mathbb{R}$ , and combining with (2.74) gives

$$\begin{aligned} & \frac{1}{Y} \int_{\log 2}^Y \left( 2 \left| \sum_{0 < |\gamma| < T} \alpha_\rho \frac{e^{i\gamma y}}{\rho(i\gamma + 1)} + \nu \right| |V(e^y)| + |V(e^y)|^2 \right) dy \\ & \ll \epsilon + \epsilon^2, \end{aligned} \tag{2.78}$$

for all  $Y$  sufficiently large. Since we may make  $\epsilon$  as small as we wish, we have that (2.75) converges to the rhs of (2.76), and is *positive* because at least one  $\alpha_\rho$  is non-zero. Hence,

$$M(e^y) = \Omega(1), \tag{2.79}$$

i.e.

$$M(x) = \Omega(1), \tag{2.80}$$

which implies, from (2.72), that

$$\Delta(x) = \Omega(1), \tag{2.81}$$

and hence from (2.71) we get (2.52).

## 2.5 Unsmoothed mean square estimate

In this subsection we give an alternate proof of the Omega bound (2.52) by working out an unsmoothed mean square.

Substituting  $y = \log x$  and  $Y = \log X$  in (2.70), we consider

$$P(e^y) - \frac{r}{\phi(q)} \pi(e^y) = \frac{e^{y/2}}{y} \left( \sum_{0 < |\gamma| < e^Y} \alpha_\rho \frac{e^{i\gamma y}}{\rho} + \nu + O \left( \frac{e^{y/2} Y^2}{e^Y} + \frac{1}{y} \right) \right). \tag{2.82}$$

Unlike  $M(x)$  which was uniformly approximated by the finite sum (2.73), the above diverges absolutely and cannot be uniformly approximated. However we can show that we can approximate the sum with finitely many terms so that the remainder term is uniformly small in mean square.

Thus, truncate the sum over  $\rho$  at some large, but fixed  $T$  (i.e. independent of  $y$ ), and consider, the mean square of the remainder. This is essentially Lemma 2.2 of [7], but we provide slightly more detail here. Thus, for  $T \geq 1$ , and  $\log 2 \leq y$ , we have

$$P(e^y) - \frac{r}{\phi(q)}\pi(e^y) = \frac{e^{y/2}}{y} \left( \sum_{0 < |\gamma| < T} \alpha_\rho \frac{e^{i\gamma y}}{\rho} + \nu + r(y, T) \right), \quad (2.83)$$

where, for all  $Y$  satisfying  $y \leq Y$ ,

$$r(y, T) = \sum_{T \leq |\gamma| < e^Y} \alpha_\rho \frac{e^{i\gamma y}}{\rho} + O\left(\frac{e^{y/2}Y^2}{e^Y} + \frac{1}{y}\right). \quad (2.84)$$

The following lemma gives a bound on the mean square of the remainder  $r(y, T)$ .

**Lemma 2.1** *Let  $T > 1$  and  $Y > T^{1/2}/\log T$ . Then,*

$$\frac{1}{Y/2} \int_{Y/2}^Y |r(y, T)|^2 dy \ll_q \frac{\log(T)^2}{T}. \quad (2.85)$$

*Proof:* Substitute (2.84) into the integrand, and use the inequality

$$|a + b|^2 \leq 2(|a|^2 + |b|^2), \quad (2.86)$$

which follows from the arithmetic geometric mean inequality  $2|ab| \leq |a|^2 + |b|^2$ , to get

$$\int_{Y/2}^Y |r(y, T)|^2 dy \ll \int_{Y/2}^Y \left| \sum_{T \leq |\gamma| \leq e^Y} \alpha_\rho \frac{e^{iy\gamma}}{1/2 + i\gamma} \right|^2 dy + 1/Y. \quad (2.87)$$

The term  $1/Y$  comes about from integrating the square of the  $O$  term in (2.82). Multiplying out the sum above by its conjugate, estimating the resulting integral, and extending the double sum to infinity, the rhs above becomes

$$\begin{aligned} & \sum_{\substack{T \leq |\gamma_1| \leq e^Y \\ T \leq |\gamma_2| \leq e^Y}} \frac{\alpha_{\rho_1} \bar{\alpha}_{\rho_2}}{\rho_1 \bar{\rho}_2} \int_{Y/2}^Y e^{iy(\gamma_1 - \gamma_2)} dy + 1/Y \\ & \ll \sum_{\substack{T \leq |\gamma_1| \leq \infty \\ T \leq |\gamma_2| \leq \infty}} \frac{1}{|\rho_1| |\rho_2|} \min \left( Y, \frac{1}{|\gamma_1 - \gamma_2|} \right) + 1/Y. \end{aligned} \quad (2.88)$$

Breaking up the sum over zeros into unit intervals  $|\gamma| \in [n, n+1)$ , with  $n \in \mathbb{Z}$ ,  $n \geq T-1$ , and using (2.64) to bound the number of such  $\gamma$  by  $O(\log m)$ , the above sum is bounded by

$$\ll Y \sum_{n \geq T-1} \frac{\log(n)^2}{n^2} + \sum_{\substack{n \geq T-1 \\ m \geq n+1}} \frac{\log m}{m} \frac{\log n}{n} \frac{1}{m-n}. \quad (2.89)$$

The first sum accounts for the contribution of the diagonal terms, i.e. where  $|\gamma_1|$  lies in an interval  $[n, n+1)$  and  $|\gamma_2|$  lies in  $[m, m+1)$ , with  $|m-n| \leq 1$ . For such pairs of zeros, which could potentially be very close, we use  $Y$  as an upper bound for  $\min(Y, 1/|\gamma_1 - \gamma_2|)$ . For all other pairs of zeros the quantity  $1/|\gamma_1 - \gamma_2| \ll 1/|m-n|$  is much smaller than  $Y$ . This gives the second sum above, i.e. the off-diagonal terms. We have also exploited symmetry in taking half the terms, i.e. we have dropped  $n \geq m+1$ .

By comparing with the integral  $\int_T^\infty \log(t)^2/t^2 dt$ , we get, on integrating by parts,

$$\sum_{n \geq T-1} \frac{\log(n)^2}{n^2} \ll \frac{\log(T)^2}{T}. \quad (2.90)$$

To bound the off-diagonal contribution, break up the sum over  $m$  into the terms,  $n+1 \leq m \leq 2n$ , and the tail  $m > 2n$ . The first portion



can be estimated as follows:

$$\sum_{\substack{n \geq T-1 \\ n+1 \leq m \leq 2n}} \frac{\log m}{m} \frac{\log n}{n} \frac{1}{m-n} \ll \sum_{n \geq T-1} \frac{\log(n)^2}{n^2} \sum_{n+1 \leq m \leq 2n} \frac{1}{m-n} \ll \sum_{n \geq T-1} \frac{\log(n)^3}{n^2} \ll \frac{\log(T)^3}{T}. \quad (2.91)$$

For the contribution from the tail, use  $1/|m-n| < 2/m$  when  $m > 2n$ :

$$\sum_{\substack{n \geq T-1 \\ m > 2n}} \frac{\log m}{m} \frac{\log n}{n} \frac{1}{m-n} \ll \sum_{n \geq T-1} \frac{\log n}{n} \sum_{m > 2n} \frac{\log m}{m} \frac{1}{m} \ll \sum_{n \geq T-1} \frac{\log(n)^2}{n^2} \ll \frac{\log(T)^2}{T}, \quad (2.92)$$

where we used  $\sum_{m > 2n} \log(m)/m^2 \ll \log(n)/n$  in passing from the second to third expression.

Putting these bounds together gives

$$\int_{Y/2}^Y |r(y, T)|^2 dy \ll_q Y \frac{\log^2 T}{T} + \frac{\log(T)^3}{T} + \frac{1}{Y}. \quad (2.93)$$

For given  $T$ , and all  $Y > T^{1/2}/\log T$ , the first term on the rhs dominates. Dividing by  $\frac{1}{Y^{1/2}}$  gives the lemma.

Returning to (2.83), we consider the mean square:

$$\frac{1}{Y/2} \int_{Y/2}^Y \left| \left( P(e^y) - \frac{r}{\phi(q)} \pi(e^y) \frac{y}{e^{y/2}} \right) \right|^2 dy = \frac{1}{Y/2} \int_{Y/2}^Y \left| \sum_{0 < |\gamma| < T} \alpha_\rho \frac{e^{i\gamma y}}{\rho} + \nu + r(y, T) \right|^2 dy. \quad (2.94)$$

The above equals

$$\frac{1}{Y/2} \int_{Y/2}^Y \left| \sum_{0 < |\gamma| < T} \alpha_\rho \frac{e^{i\gamma y}}{\rho} + \nu \right|^2 dy + E \quad (2.95)$$

where

$$|E| \ll \frac{1}{Y/2} \int_{Y/2}^Y \left| \sum_{0 < |\gamma| < T} \alpha_\rho \frac{e^{i\gamma y}}{\rho} + \nu \right| |r(y, T)| dy + \frac{1}{Y/2} \int_{Y/2}^Y |r(y, T)|^2 dy. \quad (2.96)$$

By multiplying the expression inside the absolute value of (2.95) by its conjugate, and integrating termwise, we get

$$\frac{1}{Y/2} \int_{Y/2}^Y \left| \sum_{0 < |\gamma| < T} \alpha_\rho \frac{e^{i\gamma y}}{\rho} + \nu \right|^2 dy = \nu^2 + \sum_{0 < |\gamma| < T} \frac{|\alpha_\rho|^2}{|\rho|^2} + O_T(1/Y). \quad (2.97)$$

Next we estimate  $E$ . The bound (2.96) gives

$$|E| \ll \max_{Y/2 \leq y \leq Y} \left| \sum_{0 < |\gamma| < T} \alpha_\rho \frac{e^{i\gamma y}}{\rho} + \nu \right| \left| \frac{1}{Y/2} \int_{Y/2}^Y |r(y, T)| dy + \frac{1}{Y/2} \int_{Y/2}^Y |r(y, T)|^2 dy \right|. \quad (2.98)$$

Lemma 2.1 gives an estimate for the second integral:

$$\frac{1}{Y/2} \int_{Y/2}^Y |r(y, T)|^2 dy \ll \frac{\log(T)^2}{T}. \quad (2.99)$$

Now, from (2.64)

$$\left| \sum_{0 < |\gamma| < T} \alpha_\rho \frac{e^{i\gamma y}}{\rho} + \nu \right| \ll \sum_{|\gamma| < T} \frac{1}{|\rho|} \ll \log(T)^2. \quad (2.100)$$

Furthermore, the Cauchy-Schwarz inequality gives

$$\frac{1}{Y/2} \int_{Y/2}^Y |r(y, T)| dy \ll \left( \frac{1}{Y/2} \int_{Y/2}^Y dy \int_{Y/2}^Y |r(y, T)|^2 dy \right)^{1/2}, \quad (2.101)$$

which, by lemma 2.1, is

$$\ll \frac{\log T}{T^{1/2}}. \quad (2.102)$$

Since we may choose  $T$  as large as we please, we have on combining the above estimates, that, as  $Y \rightarrow \infty$ ,

$$\frac{1}{Y/2} \int_{Y/2}^Y \left| \left( P(e^y) - \frac{r}{\phi(q)} \pi(e^y) \right) \frac{y}{e^{y/2}} \right|^2 dy \rightarrow \nu^2 + \sum_{\rho \neq 1/2} \frac{|\alpha_\rho|^2}{|\rho|^2}. \quad (2.103)$$

As in the previous subsection, the rhs above is positive because at least one of the  $\alpha_\rho$  is non-zero. Therefore,

$$\left( P(e^y) - \frac{r}{\phi(q)} \pi(e^y) \right) \frac{y}{e^{y/2}} = \Omega(1), \quad (2.104)$$

and hence

$$P(x) - \frac{r}{\phi(q)}\pi(x) = \Omega\left(\frac{x^{1/2}}{\log x}\right). \quad (2.105)$$

This establishes Theorem 1 in the case of residue classes.

Note that it is important that  $r/\phi(q) < 1$ , since if we take  $P$  to be the set of all primes then it *can* be realized, in many ways, as a union of primes in residue classes by taking all residue classes mod  $q$ , for any positive integer  $q$ . The reason the proof fails in this case is that  $P(x) - \pi(x)$  is then identically zero (and hence continuous), giving a mean square for  $P(x) - \pi(x)$ , and more precisely, of (2.103), which is always zero. The positivity of the rhs of that equation requires there to be at least one non-zero term appearing on the rhs. However, from the formula analogous to (2.37), all the  $c_\chi$  and hence  $\alpha_\rho$  are 0, and similarly for the term  $r/\phi(q) - \kappa$  which then equals 0.

### 3 Generalization to Chebotarev sets

Here we generalize the problem to prime ideals and Chebotarev sets.

Therefore, let  $L$  be a Galois extension of  $K$  with Galois group  $G = \text{Gal}(L/K)$ . For a prime ideal  $\mathfrak{p} \in K$ , we let the Artin symbol  $(L/K, \mathfrak{p})$  denote the conjugacy class of Frobenius automorphisms corresponding to the prime ideals  $\mathfrak{P} \in L$  that divide  $\mathfrak{p}$ .

Given a conjugacy class  $C$  of  $G$ , we let

$$P_{L/K, C} = \{\mathfrak{p} \in \pi(K) \mid \mathfrak{p} \text{ unramified in } L, (L/K, \mathfrak{p}) = C\}, \quad (3.1)$$

consist of the unramified prime ideals  $\mathfrak{p} \in K$ , and Frobenius conjugacy

class in  $G$  equal to  $C$ . We define the counting function

$$\pi(x, L/K, C) := \sum_{\substack{N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x \\ \mathfrak{p} \in P_{L/K, C}}} 1 \quad (3.2)$$

to be the number of prime ideals in  $P_{L/K, C}$  with norm less than or equal to  $x$ . Throughout what follows, we simply write  $N\mathfrak{a}$  rather than  $N_{K/\mathbb{Q}}(\mathfrak{a})$ .

The Chebotarev density theorem states that

$$\pi(x, L/K, C) \sim \frac{|C|}{|G|} \text{Li}(x), \quad (3.3)$$

and the prime number theorem for prime ideals in  $K$  states that

$$\pi(x, K) := \{\mathfrak{p} \in \pi(K) \mid N\mathfrak{p} \leq x\} \sim \text{Li}(x). \quad (3.4)$$

Therefore, say we have a subset  $P$  of prime ideals in  $\pi(K)$  that is realized, up to finitely many exceptions, as a finite union of Frobenius conjugacy classes in the Galois group  $G$  of some Galois extension  $L$  of  $K$ . We can restrict ourselves to the case of a single Galois extension  $L$  for similar reasons that we were able to restrict ourselves to a single modulus  $q$  in the previous section. See the comments in the introduction in Section 1.1.

### 3.1 Proof of Theorem 1 and 2

All the formulas used in the classical situation of residue classes in Section 2 have analogues in the case of number fields. In particular, the explicit formula for our situation has been worked out, with remainder terms, by Lagarias and Odlyzko [6]. We develop and collect below the needed formulas.

Define

$$\psi(x, L/K, C) := \sum_{\substack{N\mathfrak{p}^m \leq x \\ \mathfrak{p} \text{ unramified} \\ (L/K, \mathfrak{p})^m = C}} \log N\mathfrak{p}, \quad (3.5)$$

$$\begin{aligned} \Pi(x, L/K, C) &:= \sum_{\substack{N\mathfrak{p}^m \leq x \\ \mathfrak{p} \text{ unramified} \\ (L/K, \mathfrak{p})^m = C}} \frac{1}{m} \\ &= \pi(x, L/K, C) + R(x, L/K, C), \end{aligned} \quad (3.6)$$

where

$$R(x, L/K, C) := \sum_{\substack{N\mathfrak{p}^m \leq x \\ \mathfrak{p} \text{ unramified}, m \geq 2 \\ (L/K, \mathfrak{p})^m = C}} \frac{1}{m}, \quad (3.7)$$

so that

$$\begin{aligned} \pi(x, L/K, C) &= \Pi(x, L/K, C) - R(x, L/K, C) \\ &= \frac{\psi(x, L/K, C)}{\log(x)} + \int_2^x \frac{\psi(t, L/K, C)}{t \log(t)^2} dt - R(x, L/K, C). \end{aligned} \quad (3.8)$$

Likewise, define

$$\Pi(x, K) := \sum_{N\mathfrak{p}^m \leq x} \frac{1}{m} = \pi(x, K) + R(x, K), \quad (3.9)$$

where

$$R(x, K) := \sum_{\substack{N\mathfrak{p}^m \leq x \\ m \geq 2}} \frac{1}{m}. \quad (3.10)$$

Thus,

$$\begin{aligned} \pi(x, K) &= \Pi(x, K) - R(x, K) \\ &= \frac{\psi(x, K)}{\log(x)} + \int_2^x \frac{\psi(t, K)}{t \log(t)^2} dt - R(x, K). \end{aligned} \quad (3.11)$$

We will also use

$$\begin{aligned} R(x, K) &= \sum_{N\mathfrak{p}^2 \leq x} \frac{1}{2} + \sum_{\substack{N\mathfrak{p}^m \leq x \\ m \geq 3}} \frac{1}{m} \\ &= x^{1/2} / \log x + O(x^{1/3} / \log x), \end{aligned} \quad (3.12)$$

which follows from the prime number theorem for ideals, with the implied constant in the  $O$  depending on  $K$ . Similarly, from the Chebotarev density theorem, we have

$$\sum_{j=1}^r R(x, L/K, C_j) = \kappa x^{1/2} / \log x + O(x^{1/2} / \log(x)^2), \quad (3.13)$$

with the implied constant in the  $O$  depending on  $L/K$  and the  $C_j$ , and, overriding the notation for  $\kappa$  used earlier,

$$\kappa = \frac{1}{|G|} \sum_{j=1}^r |C_j| \sum_{b^2 \in C_j} 1, \quad (3.14)$$

the inner sum counting the number of conjugacy class representatives  $b \in G$  that, when squared, lie in  $C_j$ .

To obtain an explicit formula for  $\psi(x, L/K, C)$ , Lagarias and Odlyzko mimic the approach taken in Davenport for primes in arithmetic progression, using the following linear combination of logarithmic derivatives of Artin  $L$ -functions in order to extract primes ideals (and their powers) lying in the conjugacy class  $C$ :

$$\begin{aligned} F_C(s) &:= -\frac{|C|}{|G|} \sum_{\phi} \bar{\phi}(g) L'/L(s, \phi, L/K) \\ &= \sum_{\mathfrak{p}^m} \theta(\mathfrak{p}^m) \log(N\mathfrak{p}) (N\mathfrak{p})^{-ms}, \end{aligned} \quad (3.15)$$

where  $g$  is any element of the conjugacy class  $C$ ,  $\phi$  runs over the irreducible characters of  $G$ , and, for unramified  $\mathfrak{p}$ :

$$\theta(\mathfrak{p}^m) = \begin{cases} 1 & (L/K, \mathfrak{p})^m = C, \\ 0 & \text{otherwise,} \end{cases} \quad (3.16)$$

while, for ramified  $\mathfrak{p}$ ,  $|\theta(\mathfrak{p}^m)| \leq 1$ . Notice that, while the rhs of (3.15) resembles the Dirichlet series that gives the counting function in (2.25), there is a minor difference. Above, and also in (3.17) below, the

characters are primitive. The way to interpret (2.25) so that it matches with the formula here, is that each  $\chi$  in (2.25) should be replaced by its inducing character at a cost of  $O(\log(x))$  to  $\psi(x, q, a)$  coming from the primes that ramify.

Brauer [1] proved that each Artin  $L$ -function can be written as a ratio of Hecke  $L$ -functions, hence the linear combination of logarithmic derivatives of Artin  $L$ -functions above can be written in terms of Hecke  $L$ -functions. In our situation, the particular linear combination turns out, nicely, to have a similar form to (3.15). Lagarias and Odlyzko use a construction (Lemma 4.1 in their paper) of Deuring [3] to write

$$F_C(s) = -\frac{|C|}{|G|} \sum_{\chi} \bar{\chi}(g) L'/L(s, \chi, L/E), \quad (3.17)$$

where  $\chi$  runs over the irreducible Hecke characters of  $H = \langle g \rangle$ , the cyclic subgroup generated by  $g$ , and  $E$  is the fixed field of  $H$ .

The advantage of writing  $F_C(s)$  in terms of Hecke characters is that the analytic properties of Hecke  $L$ -functions are well established. Lagarias and Odlyzko carry out a Perron integral in order to extract the Dirichlet coefficients, with  $N\mathfrak{p}^m \leq x$ , of  $F_C(s)$ .

Restricting to  $2 < x < X$ , equation (7.4) of [6] gives

$$\psi(x, L/K, C) = \frac{|C|}{|G|} \left( x - \sum_{\chi} \bar{\chi}(g) \sum_{|\Im \rho_{\chi}| < X} \frac{x_{\chi}^{\rho}}{\rho_{\chi}} \right) + \text{remainder}(x, X, L/K, C), \quad (3.18)$$

where

$$\text{remainder}(x, X, L/K, C) = O \left( \frac{x \log(X)^2}{X} + \log x \right), \quad (3.19)$$

with the implied constant depending on  $L/K$  and  $C$ . Here,  $\rho$  runs over all the non-trivial zeros of  $L(s, \chi, L/E)$ . The main term  $\frac{|C|}{|G|}x$  arises

from the principal character  $\chi_0$  since  $L(s, \chi_0, L/E)$  has, up to finitely many Euler factors,  $\zeta(s)$  as one of its factors, and hence a simple pole at  $s = 1$ .

Our remainder term is simpler than in (7.4) of Lagarias and Odlyzko because we are taking  $L/K$  to be fixed. Furthermore,  $\text{remainder}(x, X, L/K, C)$  is a piecewise continuous function, with  $O(\log x)$  discontinuities at the points  $x = N\mathfrak{p}^m$ , where  $\mathfrak{p}$  runs over the ramified prime in  $K$ .

Substitute (3.18) into (3.8), apply the estimate (3.13), and then substitute all into

$$P(x) = \lambda + \sum_{j=1}^r \pi(x, L/K, C_j), \quad (3.20)$$

where  $\lambda \in \mathbb{Z}$  accounts for finitely many exceptions, and  $x$  is sufficiently large (so that  $x$  exceeds the norm of any of these exceptions). Assuming that

$$\sum_{j=1}^r |C_j|/|G| = a/b, \quad (3.21)$$

we have, on subtracting the analogous formula for  $a/b\pi(x, K)$  and cancelling the main term coming from pole at  $s = 1$  of the factor of  $\zeta(s)$  in the Dedekind zeta function  $\zeta_K$ , that, for  $2 \leq x < X$ , and assuming GRH,

$$P(x) - \frac{a}{b}\pi(x, K) = \frac{x^{1/2}}{\log x} \left( \sum_{|\gamma| < X} \alpha_\rho \frac{x^{i\gamma}}{\rho} + (a/b - \kappa) + O\left(\frac{x^{1/2} \log(X)^2}{X} + \frac{1}{\log x}\right) \right), \quad (3.22)$$

$\alpha_\rho \in \mathbb{C}$ , and where the sum over  $\rho$  is over the non-trivial zeros of all relevant  $L$ -functions, namely the Hecke  $L$ -functions, for each  $C_j$  in (3.17).

As in the classical case, if the term  $\rho = 1/2$  appears in the sum, we absorb it into the constant term. Thus, let  $\mu = a/b - \kappa$  plus, in



the event that  $\rho = 1/2$  appears in the sum,  $2\alpha_{1/2}$ . The above then becomes

$$P(x) - \frac{a}{b}\pi(x, K) = \frac{x^{1/2}}{\log x} \left( \sum_{0 < |\gamma| < X} \alpha_\rho \frac{x^{i\gamma}}{\rho} + \mu + O\left(\frac{x^{1/2} \log(X)^2}{X} + \frac{1}{\log x}\right) \right), \quad (3.23)$$

The cancellation of the main term deserves some elaboration. The  $L$ -function corresponding to the principal character in (3.17) factors as product of  $\zeta_E(s)$  and Hecke  $L$ -functions, and, because  $K \subseteq E$ ,  $\zeta_E(s)$  itself has  $\zeta_K(s)$  as a factor. The latter Dedekind zeta function is responsible for cancellation in (3.22) not just of the main term, but also of some additional terms corresponding to the non-trivial zeros of  $\zeta_K(s)$ . We therefore see that we could, in the statement of Theorem 1 replace  $\frac{a}{b}\pi(x, K)$  with  $\frac{a}{b}\pi(x, F)$ , where  $F$  is any finite extension of  $\mathbb{Q}$ , or even just  $\frac{a}{b}\text{Li}(x)$ , since these would have the same effect of cancelling the main term, with no further impact on the form of the remaining terms. Similarly, we could replace the counting function by  $Q(x)$  where  $Q$  is another Chebotarev set with the same density  $a/b$  as  $P$ .

Next, the jump discontinuities of the lhs of (3.23), up to given  $x$ , outnumber those of the  $O$  term of the rhs, for the same reason as in the case of residue classes mod  $q$ : the discontinuities of the remainder term occur at  $x = N\mathfrak{p}^m$ ,  $m \geq 2$ , for  $\mathfrak{p} \in \pi(K)$ , coming from the terms  $R(x, L/K, C_j)$  and  $R(x, K)$ , of which, because  $m \geq 2$ , there are  $O(x^{1/2}/\log x)$  many. The other discontinuities come from the ramified primes of which there are finitely many (and  $O(\log x)$  of their powers, but these powers are already counted as discontinuities of  $R(x, K)$ ). On the other hand, the lhs has jump discontinuities at all prime ideals  $\pi \in \pi(K)$  of which there are asymptotically  $x/\log x$  many. We therefore conclude, as previously, that infinitely many of the

$\alpha_\rho$  must be non-zero or else the sum over zeros would be a continuous function and the rhs would not have sufficiently many discontinuities.

Again this holds when we replace  $\frac{a}{b}\pi(x, K)$  with any of  $\frac{a}{b}\pi(x, F)$ ,  $\frac{a}{b}\text{Li}(x)$ , or  $Q(x)$  as above, though in the latter case we must also ensure that  $Q$  does not essentially coincide with  $P$ , namely that the symmetric difference  $P \triangle Q$  is infinite. In each case the difference between  $P(x)$  and any of these counting functions has discontinuities at a positive proportion of  $N\mathfrak{p}$  for primes ideals  $\mathfrak{p} \in \pi(K)$ , i.e. at  $\gg x/\log x$  points.

As in the previous Section, define

$$\Theta = \limsup\{\Re\rho | \alpha_\rho \neq 0\}. \quad (3.24)$$

Then,  $\Theta \geq 1/2$ .

If  $\Theta = 1/2$ , we have two mean square estimates analogous to those in Sections 2.4 and 2.5. In order to carry out these estimates, we also need a bound, as before, for the number of non-trivial zeros of a Hecke  $L$ -function,  $N(L, T) = |\{\rho : L(\rho) = 0, |\Im\rho| \leq T, 0 < \Re\rho < 1\}|$ , in intervals of length one. Lagarias and Odlyzko prove, in Lemma 5.4 of [6], that  $N(L, T+1) - N(L, T) = O(\log T)$ , with the implied constant depending on the  $L$ -function, hence the method used to obtain the mean square estimate in the case of Dirichlet  $L$ -functions and residue classes follows through as before and we summarize the formulas.

Adapting the notation used in Section 2.4, let

$$\Delta(x) := \frac{\log x}{x^{1/2}} \left( P(x) - \frac{a}{\phi(b)} \pi(x, K) \right). \quad (3.25)$$

and

$$M(x) := \frac{1}{x} \int_2^x \Delta(t) dt. \quad (3.26)$$

Then

$$\begin{aligned} & \lim_{Y \rightarrow \infty} \frac{1}{Y} \int_{\log 2}^Y |M(e^y)|^2 dy \\ &= \sum_{0 < |\gamma| < T} \frac{|\alpha_\rho|^2}{|\rho(i\gamma + 1)|^2} + \mu^2, \end{aligned} \quad (3.27)$$

and

$$\begin{aligned} & \lim_{Y \rightarrow \infty} \frac{1}{Y/2} \int_{Y/2}^Y \left| \left( P(e^y) - \frac{a}{b} \pi(e^y, K) \right) \frac{y}{e^{y/2}} \right|^2 dy \\ &= \mu^2 + \sum_{\rho \neq 1/2} \frac{|\alpha_\rho|^2}{|\rho|^2}. \end{aligned} \quad (3.28)$$

And, because at least one  $\alpha_\rho$  is non-zero, both mean squares are positive. From either, we can thus conclude as in Sections 2.4 or 2.5 that

$$P(x) - \frac{a}{b} \pi(x, K) = \Omega \left( \frac{x^{1/2}}{\log x} \right). \quad (3.29)$$

This concludes our proof of Theorems 1 and 2.

We also get the following theorem, depending on the value of  $\Theta$ :

**Theorem 4** *For every  $\delta > 0$ ,*

$$P(x) - \frac{a}{b} \pi(x, K) = \Omega(x^{\Theta-\delta}), \quad (3.30)$$

*with the implied constant in the  $\Omega$  depending on  $\delta$ , and  $P$ .*

**Proof:** If  $\Theta = 1/2$  then Theorem 1 provides a stronger result and the above therefore holds. If  $\Theta > 1/2$ , the theorem follows, as in Section 2.2, from the fact that at least one  $\alpha_\rho$  is non-zero and from the identity, initially derived with the assumption that  $\Re s > 1$ ,

$$\begin{aligned} & \int_1^\infty \frac{\sum_{j=1}^r \Pi(x, L/K, C_j) - \frac{a}{b} \Pi(x, K)}{x^{s+1}} dx \\ &= \frac{1}{s} \sum_{j=1}^r \sum_{\chi_j} \bar{\chi}(g_j) \log(L(s, \chi_j, L/E_j)) - \frac{a}{b} \log(\zeta_K(s)). \end{aligned} \quad (3.31)$$

where, for  $1 \leq j \leq r$ ,  $\chi_j$  runs over all the irreducible Hecke characters of  $H_j = \langle g_j \rangle$ , and  $E_j$  is the fixed field of  $H_j$ .

Finally, a similar theorem holds for a variety of counting functions. As before, let  $Q$  be a Chebotarev set with the same density  $a/b$  as  $P$ , such that the symmetric difference  $P \triangle Q$  is infinite, and  $F$  any finite extension of  $\mathbb{Q}$ . Let  $f(x)$  stand for any of  $\frac{a}{b}\text{Li}(x)$ ,  $\frac{a}{b}\pi(x, F)$ , or  $Q(x)$ . For each such choice of  $f(x)$ , the difference  $P(x) - f(x)$  can be expressed as a linear combination of explicit formulae having the same form as (3.22), though with the constant term  $a/b - \kappa$  replaced by  $-\kappa$  in the case of  $f(x) = \frac{a}{b}\text{Li}(x)$ , and by  $\kappa_2 - \kappa$ , when  $f(x) = Q(x)$ , where  $\kappa_2$  is the analogue of (3.14) for the Chebotarev set  $Q$ . Thus, defining  $\Theta_f$  to be the analogue, for a given  $f$ , of (3.24), we have the following theorem:

**Theorem 5** *Let  $f(x)$  be as in the above paragraph. Then, for every  $\delta > 0$ ,*

$$P(x) - f(x) = O(x^{\Theta_f - \delta}), \quad (3.32)$$

*with the implied constant in the  $O$  depending on  $\delta$ ,  $P$ , and  $f$ .*

**Acknowledgements:** We would like to thank Barry Mazur for raising the problem addressed in this paper. Jeffrey Lagarias provided some feedback regarding [6].

## References

- [1] Brauer, R. (1947). *On Artins  $L$ -series with general group characters*, Ann. Math. 48, 502514.
- [2] Davenport, H. (1980). *Multiplicative Number Theory*, second edition, GTM 74, Springer-Verlag, Berlin.

- [3] Deuring, M. (1934) *Über den Tschebotareffschen Dichtigkeitssatz*, Math. Ann. 110, 414-415.
- [4] Ingham, A.E. (1932). *The Distribution of Prime Numbers*, Cambridge University Press.
- [5] Lagarias, J. (1983). *Sets of primes determined by systems of polynomial congruences*, Illinois Jour. of Math., 27, 224-239.
- [6] Lagarias, J. and Odlyzko, A. (1977). *Effective versions of the Chebotarev density theorem*, in Algebraic Number Fields, Frohlich, A. (ed.), Academic Press, 409-464.
- [7] Rubinstein, M.O and Sarnak, P. (1994). *Chebyshev's Bias*, Experimental Mathematics, Vol. 3, No.3, 173-197.
- [8] Serre, J.P. (1976). *Divisibilité de certaines fonctions arithmétiques*, Enseignement Math. (2), 22, 227-260.
- [9] Serre, J.P. (2011). *Lectures on  $N_X(p)$* , A K Peters/CRC Press.